Accellion Share Securely™

AN ACCELLION WHITE PAPER

Closing the Security Gap – Extending Microsoft SharePoint, OCS, and Exchange to Support Secure File Sharing

SECURITY – COMPLIANCE – EASE OF USE

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com

Executive Summary

To compete efficiently in today's global economy, and to make the most of distributed teams, enterprises depend on online communication and collaboration.

The majority of enterprises today use Microsoft SharePoint, OCS and Exchange. But these products create security challenge for enterprises that need to collaborate with external users.

.

The majority of these enterprises today use Microsoft communication and collaboration infrastructure software including Microsoft SharePoint, OCS, and Exchange.

But these products create security challenges for enterprises that need to collaborate and share information with external users such as federated partners, customers, remote users, and mobile workers. The challenge lies in the limitations these Microsoft solutions impose on file sharing.

This whitepaper explores the challenges of secure file sharing from Microsoft SharePoint, OCS, and Exchange.

.

.

Introduction

The majority of enterprises today use Microsoft communication and collaboration infrastructure software including Microsoft SharePoint, OCS, and Exchange.

Today, Microsoft Exchange is the most prevalent email server for business. For collaboration and content management, more than 100 million users use Microsoft SharePoint. The Microsoft Office Communications Server (OCS) rounds out Microsoft's communication and collaboration solutions with a client that offers IM, telephony, voice/video conferencing, web conferencing, and other collaborative technologies.

Enterprises need more flexibility, including the ability to transfer files securely to users outside the firewall, who lack access to an internal SharePoint server.

Together, these Microsoft products make it easy for enterprise users to communicate and collaborate. Users can switch easily from email to chat to blogging to VOIP conferencing, using whatever tool best meets their collaboration needs at the moment.

But these products create security challenges for enterprises that need to collaborate and share information with external users such as federated partners, customers, remote users, and mobile workers.

The challenge lies in the limitations these Microsoft solutions impose on file sharing. Enterprises need more flexibility, including the ability to transfer files securely to users outside the firewall who lack access to an internal SharePoint server. Enterprises need to be able to reach these users without setting up complex external server farms and punching holes in firewalls. Enterprises also need security and audit controls lacking in Exchange and OCS.

The Security Gap Between File Sharing Capabilities and Communication and Collaboration Requirements

All three Microsoft communication and collaboration solutions—Exchange, SharePoint, and OCS—offer some means of file sharing:

- SharePoint offers a secure data repository that enterprises can use to manage and protect confidential files. Users can upload files into SharePoint Document Libraries where only authorized users can access them.
- OCS, like other IM applications, includes a file transfer mechanism that enables users to send a file to other users, such as colleagues participating in a chat or video session.
- Exchange enables users to send files as email attachments.

But these products, by themselves, don't meet the need of today's agile, highly distributed organizations. Today, internal users need to collaborate not only with one another, but also with a broad community of external users, including

- Partners
- Customers

- Consultants
- Remote users
- Foreign manufacturers
- Remote divisions and branch offices
- Law offices
- PR and marketing agencies
- Industry consortia

To collaborate effectively, internal users need a way to easily and securely transfer files to these external users. They need to bridge the security gap in their communication and collaboration infrastructure to reach larger, heterogeneous communities of collaborators.

To collaborate effectively, internal users need a way to easily and securely transfer files to external users.

Simply finding a way to transfer files isn't enough–enterprises must ensure that file transfers are secure. IT managers and security officers need to audit file transfers and confirm that confidential data is not being sent to inappropriate parties. File transfers must comply with all applicable laws and industry regulations mandating security and audit trails for confidential communications. Applicable laws and regulations might include Sarbanes-Oxley (SOX), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Availability Act (HIPAA).

Let's examine how the security gap affects each solution in the Microsoft communication and collaboration infrastructure: SharePoint, OCS, and Exchange.

The Security Gap in SharePoint

SharePoint's security is based on authorized users (usually employees) checking files into and out of secured Document Libraries. To share files, internal users share links that work only within the SharePoint domain. These links don't work for external users.

It's rare for an IT department to give SharePoint accounts to external users for sharing information. It is extremely cumbersome and expensive to set up access and manage separate servers in the DMZ. Because external users are blocked from SharePoint access, internal SharePoint users cannot easily or securely transfer files to large numbers of users with whom they're collaborating.

Dangerous Workarounds and the Risk to Compliance

When users discover they can't share their SharePoint files with external users, they frequently seek workarounds, regardless of the security risks. After all, one way or another, they need to share files. So users resort to emailing files through a personal webmail account, sign up for a free file-sharing service, or to copy the files to a USB memory stick or a CD ROM.

In all these cases, files are transferred in unsecure ways outside of the purview of the IT department. The enterprise loses control and oversight over the files.

Security risks abound. Email may be forwarded or intercepted. File-sharing services may leave confidential files vulnerable on servers. USB memory sticks and CD ROMs may be lost. If the files contain confidential data, such transfers may violate privacy laws and industry regulations.

An Expensive Alternative: Building an In-house File Transfer Server Farm

To protect, track, and manage files exchanged through ad hoc collaborations with employees and outside federated partners, enterprises need to close the security gap in Microsoft's communication and collaboration infrastructure.

To bridge this security gap, an enterprise can set up dedicated file servers with authentication systems for external users. IT can set up external-facing SharePoint servers and change network topologies to create a secure environment for external communications.

But this is expensive, time-consuming, and cumbersome—a real IT nightmare. Few enterprise IT departments would seriously consider taking on this sort of overhead, which involves capital expenses, considerable software licensing costs, and ongoing labor costs. The very idea of exposing confidential data sources is likely to make security and compliance officers uneasy. To mitigate one set of security risks, this approach creates another set, and requires a significant hardware investment as well.

The Security Gap in OCS

A different file transfer security gap affects communications through OCS. The risk here is that files can be readily transferred in unsecure ways and without IT knowledge. Sufficient encryption and authentication controls are not in place.

Microsoft Office Communications Server R2, for example, allows users to transfer files to any other user of OCS, a federated partner or a user of PIC-compatible IM client (such as Yahoo!, MSN, and AOL clients). Enterprise IT has to open ports on the firewalls for the information sharing in Microsoft OCS R2. There's no easy way for IT to ensure that files are being transferred securely and in compliance with company policies. The file transfers are unencrypted, unmonitored, and not auditable.

To protect, track, and manage files exchanged through ad hoc collaborations with employees and outside federated partners, enterprises need to close the security gap in Microsoft's communication and collaboration infrastructure. They need a secure file transfer solution that complements and extends the Microsoft infrastructure, enabling users to continue using the client and server programs they're familiar with, while taking advantage of encryption, authentication, and other security mechanisms for protecting valuable data assets.

The Security Gap in Exchange

A similar problem of unsecure and unsupervised file transfer exists for Microsoft Exchange. Sending file attachments is second nature for email users. The ease with which email can be used to send attachments has made it the most commonly used file transfer mechanism for business users today. While sending files through email is very convenient, email systems were never designed to handle file attachments efficiently or securely. The enormous volume of information being sent in email attachments has resulted in degraded email server performance, slower message delivery times and security concerns. Because as much as 80% of email storage is files, addressing the performance and security issues related to file transfers is becoming increasingly critical for IT administrators and security officers.

A common practice in most organizations today is to limit the size of file attachments and place a quota on mailbox size. Unfortunately this solution for reducing the volume of files being shared via email has only increased the security concerns as business users seek unsecure IT workarounds. Use of USB sticks, unsecure FTP, P2P file sharing and shipping information on CDs via courier, as a workaround to email attachment limits, has led to many high profile data breaches.

Closing the Security Gap with Secure File Sharing

To address the security and monitoring requirements of enterprises relying on Microsoft for their communication and collaboration needs, organizations should look for a secure file transfer solution that extends the file sharing capabilities of these applications.

The Accellion Microsoft Business Productivity Suite

The Accellion Microsoft Productivity Business suite augments Microsoft Exchange, SharePoint, and OCS with secure file transfer capabilities, including features for monitoring and auditing file transfer activities.

The suite includes:

- Microsoft SharePoint 2007/2010 plug-in
- Microsoft OCS R2 plug-in
- Microsoft Outlook 2007/2010 plug-in

By deploying the Accellion solution, enterprise IT departments can ensure their users communicate and collaborate securely with both internal users and external users, while avoiding risky file-sharing practices, and avoid expensive deployments of special server farms.

The Accellion Microsoft Productivity Business suite augments Exchange, SharePoint, and OCS with secure file transfer capabilities.

MICROSOFT SHAREPOINT 2007/2010 PLUG-IN

The Accellion Microsoft SharePoint 2007/2010 plug-in is a server-based plug-in that adds Secure File Transfer capabilities to SharePoint. Users can use the plug-in to transfer files securely to other SharePoint users, in addition to authorized users, outside SharePoint infrastructure.

MICROSOFT OUTLOOK 2007/2010 PLUG-IN

The Accellion plug-in for Microsoft Outlook adds a Secure File Transfer option to the Microsoft Outlook interface. A user who wants to send files securely, simply clicks on the Accellion Secure File Transfer icon in Outlook and attaches files up to 2 GB in size.

MICROSOFT OCS R2 PLUG-IN

The Accellion OCS plug-in offers the same secure file transfer features for Microsoft OCS. Users can be engaged in OCS activity—chatting, conferencing, and etc—and transfer a file securely by clicking a button and uploading a file.

Summary

The Accellion Microsoft Business Productivity Suite offers enterprises the following benefits:

- Secure file transfer with internal users, as well as partners, customers, and other authorized external users.
- Real-time, on-demand file sharing—useful for document reviews and other collaborative processes.
- A single solution that extends all Microsoft communication and collaboration products, including SharePoint, OCS R2, and Exchange.
- Dashboard controls and reporting enabling IT managers and security officers to track the distribution of files.
- Controls for achieving compliance with SOX, HIPAA, GLBA, and internal security guidelines.
- File transfer security that extends beyond the enterprise firewall, and supports users of non-Microsoft, PIC-compatible clients.
- Return receipts through email so that users can confirm that their files have been received.

Accellion File Sharing solutions are used by leading enterprise organizations including Procter & Gamble; Activision; Indiana University Health; Kaiser Permanente; Foley & Mansfield; Lovells; Bridgestone; Ogilvy & Mather; Harvard University; Guinness World Records; US Securities and Exchange Commission; and NASA.

For more information, please visit www.accellion.com or call +1 650-485-4300.

www.accellion.com info@accellion.com

THIS DOCUMENT IS PROVIDED "AS IS." ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.